CLAIM + DETAILED DESCRIPTION

[Claim(s)]

[Claim 1]When performing access to a portable information storage medium from an external device characterized by comprising the following, are an authentication method which checks that said portable information storage medium is a right thing, and the arbitrary data R for attestation is received, So that the same data as said data R for attestation may be obtained by obtaining code data C by performing encipherment arithmetic using the 1st key alpha, and performing a decoding operation using the 2nd key beta to this code data C, While making said 1st key alpha remember it to be the operation definition stage of defining the 1st key alpha, key beta, encipherment arithmetic, and decoding operation in [portable / said] an information storage medium, [2nd] A medium preparatory step which prepares a processing capability which performs said encipherment arithmetic for said portable information storage medium, A random number transmission stage story which generates a random number in said external device, and transmits to said portable information storage medium by using this random number as the data R for attestation, A data storage stage for attestation of making the predetermined memory location in [portable / said] an information storage medium memorizing this in response to transmission of the data R for attestation, and inside of an information storage medium portable [said].

case the newly transmitted data R for attestation investigates whether it is in agreement with the data R for attestation memorized until now and its any are inharmonious -- encryption -- permission -- a judgment stage of judging.

in said judgment stage -- encryption -- permission, when a judgment is performed in [portable / said] an information storage medium, An encryption stage of performing said encipherment arithmetic using said 1st memorized key alpha to the transmitted data R for attestation, and making code data C obtained as a result replying said external device.

A decoding stage of performing said decoding operation using said 2nd key beta in said

external device to code data C replied from said portable information storage medium.
An attestation stage of checking said portable information storage medium with a right thing when the data same as a result of said decoding operation as the data R for attestation transmitted on said random number transmission stage story is obtained.

[Claim 2][in the authentication method according to claim 1] [data / R / which was transmitted by random number transmission stage story / for attestation] performing a judgment stage in advance of a data storage stage for attestation, and setting in this judgment stage -- encryption -- permission -- an authentication method of a portable information storage medium characterized by performing a data storage stage for attestation only when a decision result is obtained.
[Claim 3]In the authentication method according to claim 1 or 2, prepare two or moren memory location which can memorize the data R for attestation in [portable] an information storage medium, and, [a data storage stage for attestation] An authentication method of a portable information storage medium characterized by making it make the data R for attestation for n times memorize these days.
[Claim 4]When the data R for attestation has been transmitted with an authentication command from an external device characterized by comprising the following, A portable information storage medium with a function which performs predetermined encipherment arithmetic to this data R for attestation, and is replied to said external device by making into a response code data C obtained as a result.
A command reception part which receives a command transmitted from said external device.
A data storage part for attestation for memorizing said data R for attestation.
A secret-key storage part for memorizing secret-key alpha for using for said encipherment arithmetic.
When said command reception part receives the data R for attestation with an authentication command, An inharmonious check part which checks that the data R for attestation memorized in said data storage part for attestation and the newly received data R for attestation are inharmonious, A data write part for attestation which writes the data R for attestation which said command reception part received in said data storage part for attestation, Secret-key alpha memorized in said secret-key storage part on condition that disagreement was checked in said inharmonious check part is used, An encipherment arithmetic part which performs encipherment arithmetic to the newly received data R for attestation, and obtains code data C, and a response transmission section which transmits a response containing said code data C to said external device.

[Claim 5]It is carried out on condition that disagreement was checked in an inharmonious

check part about the newly received data R for attestation in the portable information storage medium according to claim 4, A portable information storage medium, wherein writing of said newly received data R for attestation in a data write part for attestation is performed.
[Claim 6]In the portable information storage medium according to claim 4 or 5, [a data storage part for attestation] Prepare two or moren memory location so that the data R for attestation along which it passes two or moren can be memorized, and, [a data write part for attestation] A portable information storage medium performing processing which writes the data R for attestation used as a write object in each memory location one by one, and performing rewriting processing to the memory location in which the data R for attestation in which two or moren memory location is the oldest when finishing [already / writing] altogether is written.

[Detailed Description of the Invention]
[0001]
[Field of the Invention]When accessing this invention from an external device to an IC card especially about a portable information storage medium and an authentication method for the same, it relates to an IC card suitable for performing the authentication method and such an authentication method for attesting that this IC card is a right thing.
[0002]
[Description of the Prior Art]It is also already a question of time that the portable information storage medium represented by the IC card is spreading quickly with the miniaturization technology of an IC chip, and one sheet comes to spread even round ordinary individual users at a time. Thus, the more portable information storage media, such as an IC card, come to be used as a tool which makes the base of social life, the more reservation of security serves as an important technical problem. What is called a reader writer device will be used for access to an IC card, and a computer system will carry out an exchange of the inside of an IC card, and data to it via this reader writer device. Then, if an IC card is inserted in a reader writer device, processing which attests a partner will usually be performed mutually.
[0003][the attestation for seeing an IC card from the reader writer device side, and checking whether the IC card concerned is a right thing] Usually, the arbitrary data for attestation (the random number is used) is given from a reader writer device to an IC card with an authentication command, and the right response to this is performed by the method of verifying whether it coming on the contrary. Using a public-key crypto system, more specifically, [a regular IC card] In the inside of an IC card to the data for attestation (arbitrary random numbers) which stores secret-key alpha in the inside and was given from the reader writer device side, Make the encryption processing using this secret-key alpha carry out, make the code data obtained by this encryption processing return as a response, and, [the reader writer

device side] To the code data returned as this response, decoding processing using public key beta corresponding to secret-key alpha is performed, and the data obtained by this decoding processing is performing attestation over an IC card by whether it is in agreement with the data for attestation of a basis.

[0004]Since secret-key alpha stored in the IC card usually has structure which is not read to the exterior by any methods, it is very difficult to forge the IC card which has right secret-key alpha. Therefore, by the method mentioned above, code data is made to return as a response, and if the data obtained by decrypting this is in agreement with the original data for attestation, attestation that the IC card concerned is regular will be acquired.

[0005]

[Problem to be solved by the invention]As mentioned above, logically, secret-key alpha stored in the IC card is the structure which is not read to the exterior by any methods. However, actually, it is analyzing various physical phenomena (for example, consumed electric current) under IC card operation, and the method of detecting nondestructively secret-key alpha stored in the IC card from the outside exists. For example, the technique currently called DPA (Differential Power Analysis) is based on the principle of guessing the contents of secret-key alpha, by analyzing the waveform of the power consumption of an IC card statistically. Change into the state where the system of measurement for measuring the consumed electric current in the inside of an IC card was connected, and repeating transmission of the predetermined data for attestation is specifically carried out to the terminal for electric power supplies of an IC card, etc. from the reader writer device side, The contents of secret-key alpha are grasped by a statistical technique by performing encipherment arithmetic using secret-key alpha inside an IC card, and analyzing the power consumption waveform at this time.

[0006]Then, an object of this invention is to provide the authentication method of the portable information storage medium which can secure sufficient security also to an unjust analytic method which was mentioned above.

[0007]

[Means for solving problem](1) In the authentication method which checks that this portable information storage medium is a right thing when the 1st mode of this invention performs access to a portable information storage medium from an external device, To the arbitrary data R for attestation, by performing encipherment arithmetic using the 1st key alpha, code data C is obtained and this code data C is received, So that the same data as the original data R for attestation may be obtained by performing the decoding operation using the 2nd key beta, While making the 1st key alpha remember it to be the operation definition stage of defining the 1st key alpha, key beta, encipherment arithmetic, and decoding operation in [portable] an information storage medium, [2nd] The medium preparatory step which prepares the processing capability which performs encipherment arithmetic for this portable information

storage medium, The random number transmission stage story which generates a random number in an external device and transmits to a portable information storage medium by using this random number as the data R for attestation, It is investigated whether in response to transmission of the data R for attestation, it is in agreement with the data R for attestation in which the data R for attestation newly transmitted into [portable] an information storage medium is remembered to be the data storage stage for attestation of making the predetermined memory location in [portable] an information storage medium memorizing this until now, case any are inharmonious -- encryption -- permission -- in the judgment stage of judging, and this judgment stage -- encryption -- permission, when a judgment is performed in [portable] an information storage medium, In the encryption stage of performing encipherment arithmetic using the 1st memorized key alpha to the transmitted data R for attestation, and making code data C obtained as a result replying an external device, and an external device, The decoding stage of performing the decoding operation using the 2nd key beta to code data C replied from the portable information storage medium, When the data same as a result of this decoding operation as the data R for attestation transmitted on the random number transmission stage story is obtained, it is made to perform the attestation stage of checking a portable information storage medium with a right thing.

[0008](2) In the authentication method of the portable information storage medium which requires the 2nd mode of this invention for the 1st above-mentioned mode, performing a judgment stage in advance of the data storage stage for attestation, and setting in this judgment stage about the data R for attestation transmitted by the random number transmission stage story, -- encryption -- permission -- only when a decision result is obtained, it is made to perform the data storage stage for attestation.

[0009](3) In the authentication method of the portable information storage medium which requires the 3rd mode of this invention for the 1st or 2nd above-mentioned mode, In [portable] an information storage medium, two or more Memory locationn which can memorize the data R for attestation is prepared, and it is made to make the data R for attestation for n times memorize in the data storage stage for attestation these days.

[0010](4) When the data R for attestation has been transmitted with the authentication command from the external device, [the 4th mode of this invention] In a portable information storage medium with the function which performs predetermined encipherment arithmetic to this data R for attestation, and is replied to an external device by making into a response code data C obtained as a result, The command reception part which receives the command transmitted from an external device, and the data storage part for attestation for memorizing the data R for attestation, When the secret-key storage part and command reception part for memorizing secret-key alpha for using for encipherment arithmetic receive the data R for attestation with an authentication command, The inharmonious check part which checks that

the data R for attestation memorized in the data storage part for attestation and the newly received data R for attestation are inharmonious, The data write part for attestation which writes the data R for attestation which the command reception part received in the data storage part for attestation, The encipherment arithmetic part which performs encipherment arithmetic to the newly received data R for attestation, and obtains code data C using secret-key alpha memorized in the secret-key storage part on condition that disagreement was checked in the inharmonious check part, The response transmission section which transmits the response containing code data C to an external device, ******** -- it is made like.

[0011](5) In a portable information storage medium which requires the 5th mode of this invention for the 4th above-mentioned mode, On condition that disagreement was checked in an inharmonious check part about the newly received data R for attestation, writing of the newly received data R for attestation in a data write part for attestation is made to be performed.

[0012](6) In a portable information storage medium which requires the 6th mode of this invention for the 4th or 5th above-mentioned mode, Two or moren memory location is prepared for a data storage part for attestation so that the data R for attestation along which it passes two or moren can be memorized, Perform processing for which a data write part for attestation writes the data R for attestation used as a write object in each memory location one by one, and when finishing [already / writing] altogether, [two or moren memory location] It is made to perform rewriting processing to the memory location in which the oldest data R for attestation is written.

[0013]

[Mode for carrying out the invention]Hereafter, it explains based on an embodiment illustrating this invention. First, a basic principle of an authentication method currently performed in the conventional common portable information storage medium (specifically IC card) is explained, referring to a block diagram of drawing 1. This authentication method is an authentication method using a public-key crypto system using a pair key which consists of a secret key and a public key.

[0014]In the state where inserted the portable information storage medium (IC card) 100 in the external device (reader writer device) 200, and both were electrically connected, drawing 1 is a block diagram showing the procedure which attests the IC card 100 side from the reader writer device 200 side. In the example of illustration, in IC card 100, the 1st key alpha (secret key) is stored beforehand, and the 2nd key beta (public key) is beforehand stored in the reader writer device 200. Here, the 1st key alpha is a key peculiar to the owner of this IC card 100, and is a secret key which generally is not told, for example. On the other hand, although the 2nd key beta is same key peculiar to this owner, it is the key generally exhibited. Therefore, even if it always does not store the 2nd key beta in the reader writer device 200, and it makes it read

from somewhere else (for example, host computer etc.) in the reader writer device 200 each time, it is not cared about. IC card 100 is equipped with the function to perform encryption processing to arbitrary data, using the 1st key alpha, and the reader writer device 200 is equipped with the function to perform decoding processing to arbitrary code data, using the 2nd key beta.

[0015]The reader writer device 200 is equipped with the function to generate a random number, and the random number generated with the reader writer device 200 will be transmitted to the IC card 100 side with an authentication command as the data R for attestation. In the IC card 100 side, code data C is generable by performing encipherment arithmetic using the 1st key alpha to the data R for attestation transmitted in this way. In the premise of using the 1st key alpha, code data C is data which can be uniquely found based on the data R for attestation. IC card 100 replies code data C for which it asked in this way to the reader writer device 200 as a response to an authentication command. In the reader writer device 200 side, a decoding operation is performed to code data C transmitted in this way using the 2nd key beta. And if the data obtained by this decoding operation is in agreement with the original data R for attestation, it will attest IC card 100 as a right thing.

[0016]Of course, in order to make such an authentication method possible, it is necessary to provide the 1st key alpha, 2nd key beta, encipherment arithmetic, and decoding operation in a specific thing beforehand. Namely, to the arbitrary data R for attestation, by performing encipherment arithmetic using the 1st key alpha, code data C is obtained and this code data C is received, By performing the decoding operation using the 2nd key beta, the 1st key alpha, key beta, encipherment arithmetic, and decoding operation must be defined so that the same data as said data R for attestation may be obtained. [2nd] If another word is carried out. [the 1st key alpha and the 2nd key beta] It is necessary to have a relation of the pair key equivalent to the secret key and public key in a public-key crypto system. The decoding operation performed by the encipherment arithmetic [which is performed by the IC card 100 side] and reader writer device 200 side needs to be the encipherment arithmetic and the decoding operation in this public-key crypto system.

[0017]As the data R for attestation generated in the reader writer device 200 side, since a random number is used, the contents of the data R for attestation given to the IC card 100 side will differ each time. Therefore, the contents of code data C returned as a response from the IC card 100 side also differ each time. However, if a right decoding operation is performed using right public key beta by the reader writer device 200 side as long as the IC card 100 side is carrying out right encipherment arithmetic using right secret-key alpha, decrypted data is in agreement with the original data R for attestation. Therefore, no matter the original data R for attestation may be what value, attestation over IC card 100 is attained. And since secret-key alpha stored in IC card 100 is not read to the exterior of an IC card, it looks [secure / once /

sufficient security] logical.

[0018]However, if the technique of analyzing the consumed electric current of an IC card statistically is used in fact as already stated, it will become possible to perceive the contents of secret-key alpha in IC card 100 from the outside. For example, the data R for attestation "11111111" Becoming is repeated repeatedly, and it gives IC card 100, and when a power consumption waveform of IC card 100 inside at that time is repeated and observed by an electric measuring method, a certain pattern will be obtained statistically. Similarly the data R for attestation "00000000" Becoming is repeated repeatedly, and it gives IC card 100, and when a power consumption waveform of IC card 100 inside at that time is repeated and observed by an electric measuring method, a certain pattern will be obtained statistically too. By analyzing such a pattern, it becomes possible to guess statistically the contents of secret-key alpha stored in an inside.

[0019]In order to make such an unjust analytic method difficult, the feature of this invention is at the point of refusing the encipherment arithmetic in IC card 100 inside, when the same data R for attestation is repeatedly given to IC card 100. For example, supposing the data R for attestation which it "11111111" Comes to set to the 1st authentication command is given in the case of an above-mentioned example, this 1st authentication command is received, Although encipherment arithmetic using secret-key alpha will be performed and obtained code data C will be replied as a response, When the data R for attestation which it "11111111" [same] Comes to set to the authentication command for the and afterwards time is given, the authentication command concerned will be refused and encipherment arithmetic using secret-key alpha will be performed. Of course, a normal response is not obtained, either.

[0020]Since it becomes impossible to carry out repeat execution of the encipherment arithmetic using the same data R for attestation if such structure is used, it becomes difficult to analyze a power consumption waveform by a statistical technique.

[0021]What is necessary is just to carry out composition of IC card 100 to composition as shown in the block diagram of drawing 2, in order to attain such a purpose. The block diagram of this drawing 2 shows the state where IC card 100 (portable information storage medium) concerning this invention was connected to the conventional common reader writer device 200 (external device). IC card 100 concerning this embodiment has the command reception part 110, the data write part 120 for attestation, the data storage part 130 for attestation, the inharmonious check part 140, the encipherment arithmetic part 150, the secret-key storage part 160, and the response transmission section 170 as illustration. On the other hand, the reader writer device 200 has the command transmission section 210, the data generating part 220 for attestation, the response receive section 230, the decoding operation part 240, the public key storage part 250, and the authentication section 260. Of course, only the component required in order to perform authenticating processing concerning this invention is illustrated by

drawing 2, and it is equipped with other components for performing the original function as an IC card and a reader writer device in an actual IC card and reader writer device.

[0022]The reader writer device 200 shown in drawing 2 is the conventional common reader writer device, and if it says conversely, when carrying out this invention, the reader writer device can use the conventional thing as it is. The data generating part 220 for attestation is a means to generate a random number in fact, and the random number generated here will be given to the IC card 100 side as the data R for attestation. That is, the data R for attestation generated as a random number is transmitted towards the command reception part 110 from the command transmission section 210 with an authentication command. When the data R for attestation has been transmitted with the authentication command in this way, [IC card 100] It is a portable information storage medium with the function to reply as a response code data C which performs predetermined encipherment arithmetic to this data R for attestation, and is obtained as a result, Code data C as a response will be transmitted towards the response receive section 230 from the response transmission section 170.

[0023]In the reader writer device 200 side, the decoding operation to code data C replied in this way is performed. That is, in the decoding operation part 240, the decoding operation to code data C is performed using public key beta stored in the public key storage part 250. When the decode data obtained as this result of an operation is compared with the data R for attestation of the origin which the data generating part 220 for attestation generated in the authentication section 260 and both are in agreement, the point that attestation that IC card 100 is a right thing is performed is as having already stated.

[0024]It is as on the other hand having also already described fundamentally processing of encipherment arithmetic performed by the IC card 100 side. That is, the data R for attestation received in the command reception part 110 is given to the encipherment arithmetic part 150, and is enciphered. Secret-key alpha is stored in the secret-key storage part 160. The encipherment arithmetic part 150 reads secret-key alpha from this secret-key storage part 160, performs encipherment arithmetic to the data R for attestation using this, and performs processing which asks for code data C. Code data C which was able to be found is transmitted as a response from the response transmission section 170.

[0025]However, in order for the encipherment arithmetic part 150 to perform this encipherment arithmetic, permission from the inharmonious check part 140 is needed. Unless a signal of a purport that encipherment arithmetic about this data R for attestation is permitted will be given from the inharmonious check part 140 even if the data R for attestation is given to the command reception part 110 if another word is carried out, the encipherment arithmetic part 150 will not perform encipherment arithmetic. It judges whether the data R for attestation of the inharmonious check part 140 newly given to the command reception part 110 corresponds with the data R for attestation given in the past, and only when inharmonious, a signal of a purport

that encipherment arithmetic is permitted to the encipherment arithmetic part 150 is given. In order to make such a judgment perform in the inharmonious check part 140, it is necessary to store the data R for attestation given until now. Such accumulation processing is performed by the data write part 120 for attestation, and the data storage part 130 for attestation. The data storage part 130 for attestation has the memory location for carrying out accumulation memory of two or more data R for attestation given so far, and the data write part 120 for attestation performs processing which writes the data R for attestation which the command reception part 110 received one by one in this data storage part 130 for attestation.

[0026]Of course, when using this IC card 100 for the first time. Although the data R for attestation has not been stored yet into the data storage part 130 for attestation, whenever the data R for attestation is transmitted with an authentication command from the command transmission section 210, with the data write part 120 for attestation, This data R for attestation will be written in the data storage part 130 for attestation. When the command reception part 110 receives the data R for attestation with an authentication command, [the inharmonious check part 140] It will check that the data R for attestation memorized in the data storage part 130 for attestation and the newly received data R for attestation are inharmonious, and the signal of the purport that encipherment arithmetic is permitted to the encipherment arithmetic part 150 will be given. The encipherment arithmetic part 150 performs the operation which performs encipherment arithmetic to the newly received data R for attestation, and obtains code data C using secret-key alpha memorized in the secret-key storage part 160 on condition that disagreement was checked in this inharmonious check part 140.

[0027]In this embodiment, the data write part 120 for attestation is made to write in this newly received data R for attestation, on condition that disagreement was checked in the inharmonious check part 140 about the newly received data R for attestation. Namely, when the new data R for attestation is received by the command reception part 110 with an authentication command, First, only when processing of the inharmonious check by the inharmonious check part 140 is performed and disagreement is checked, the data R for attestation concerned will be written in the data storage part 130 for attestation by the data write part 120 for attestation. Conversely, when saying and coincidence is checked in the inharmonious check part 140, the data R for attestation concerned is not written in by the data write part 120 for attestation. When such employment eliminates redundancy from the data in the data storage part 130 for attestation, it is meaningful. That is, writing for the second time is not performed about the same data as the data already memorized in the data storage part 130 for attestation.

[0028]Practically, memory space in IC card 100 is limited, and, naturally its storage capacity of the data storage part 130 for attestation is also limited. Therefore, if IC card 100 will be used for a long period of time, will be inserted in the reader writer device 200 repeatedly and will

receive attestation, void areas in the data storage part 130 for attestation will decrease in number gradually, and the data R for attestation will be soon written in all the fields. In such a case, what is necessary is to leave the latest data R for attestation and just to perform processing which is rewritten from old data in the data storage part 130 for attestation. For example, what is necessary is just to make it the data R for attestation for n times memorized recently, when two or moren memory location which can memorize the data R for attestation is prepared in the data storage part 130 for attestation. Namely, what is necessary is just to perform rewriting processing to the memory location in which the oldest data R for attestation is written, after it performs processing which writes the data R for attestation used as a write object in each memory location one by one and it already becomes finishing altogether writing in two or moren memory location until a void area is lost.

[0029]Drawing 3 is a figure showing an example of such rewriting processing. First, as shown in drawing 3 (a), when two or moren memory location shown by the memory location number 1 - n is prepared, supposing three data for attestation R (1), R (2), and R (3) are given one by one, These data will be written in the memory location numbers 1, 2, and 3 one by one as illustration. It enables it for the pointer P to have shown the last write-in place here. Then, what is necessary is to perform writing to the memory location number 4 located in the next of a write-in place of the last to which the pointer P points, and just to update the pointer P, when the new data R (4) for attestation is given for example. Drawing 3 (b) is carried out in this way, writes in one by one, and shows the state where a total of n data for attestation R (1) - R (n) were written in altogether. What is necessary is just to perform rewriting to a position of the memory location number 1 where the oldest data R (1) for attestation was written in in this state, as shown in drawing 3 (c) when the following data R for attestation (n+1) is given. Drawing 3 (d) shows write states when the still newer data R (n+2) and R for attestation (n+3) is given. Whenever it performs such rewriting processing, accumulation memory of the n newest data for attestation will be carried out.

[0030]Drawing 4 is a flow chart showing the procedure of the authentication method of the portable information storage medium concerning this invention. Of course, when carrying out the procedure shown in this drawing 4. Predetermined secret-key alpha needs to be stored and it is necessary to prepare a portable information storage medium (IC card 100) with the function to perform predetermined encipherment arithmetic using this secret-key alpha, and to prepare the external device (reader writer device 200) for accessing this.

[0031]Now, if IC card 100 is inserted in the reader writer device 200, first, in Step S1, by the reader writer device 200 side, the data R for attestation (random number) will be generated, and this data R for attestation will be transmitted to the IC card 100 side in continuing Step S2. In fact, as mentioned above, the data R for attestation will be given with an authentication command to the IC card 100 side. In Step S4 which will continue if IC card 100 receives this

data R for attestation in Step S3, A coincidence decision with the data R for attestation for the past n times is performed (what is necessary is just to, perform a coincidence decision with the data R for attestation stored until now, of course, when the data R for attestation for n times has not been stored yet into the data storage part 130 for attestation).

[0032]Here, if the judgment of the purport that any of the data R for attestation stored are inharmonious is made, it will progress to Step S6 from Step S5, and processing which writes this newly received data R for attestation in the data storage part 130 for attestation will be performed. Thus, only when the coincidence decision of Step S4 was performed and an inharmonious decision result was obtained in advance of the writing processing of the data for attestation of Step S6, as it mentioned above that it was made to perform writing processing of Step S6, It is for eliminating the redundancy of the data R for attestation stored into the data storage part 130 for attestation (in order for the same data to overlap and to make it not written in). Next, in Step S7, encipherment arithmetic using secret-key alpha is performed to this data R for attestation, and obtained code data C is transmitted as a response in Step S8.

[0033]In Step S9, the reader writer device 200 receives code data C transmitted as this response, and performs the decoding operation using public key beta to this code data C in Step S10. And in Step S11, coincidence with the decode data obtained as a result of this decoding operation and the original data R for attestation (random number by which it was generated at Step S1) is judged. If both are in agreement, it progresses to Step S13 from Step S12, it becomes an authentication success and both are not in agreement, it progresses to Step S14 from Step S12, and becomes an authentication failure. [0034]The result of the coincidence decision of Step S4 carried out on the other hand at the IC card 100 side, If the result which shifts and is in agreement with that data R for attestation to be accumulated into the data storage part 130 for attestation is obtained, it will progress to Step S15 from Step S5, and transmission of errors will be performed as a response to the reader writer device 200. In this case, in Step S16, since the reader writer device 200 will receive an error as a response, it is made to perform predetermined error handling in continuing Step S17.

[0035]If such a procedure is made to perform attestation over IC card 100, Since encipherment arithmetic [in / only within a case where the data R for attestation for the past n times is inharmonious /, in the newly given data R for attestation / Step S7] will be performed in a judgment in Step S4, The same data R for attestation can be repeated and given to IC card 100, power consumption at that time can be repeated and observed, and operation of an unjust analytic method of guessing secret-key alpha with a statistical technique can be made difficult.

[0036]As mentioned above, although it explained based on an embodiment illustrating this invention, this invention is not limited to this embodiment and is feasible with various forms. For example, to a common portable information storage medium, although an above-

mentioned embodiment described an example which performs attestation over an IC card via a reader writer device, this invention can be widely applied, when performing attestation from an external device.

[0037]

[Effect of the Invention]According to the authentication method of the portable information storage medium applied to this invention as above, it becomes possible to secure sufficient security also to an unjust analytic method.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－281019
（P2002－281019A）
(43)公開日　平成14年９月27日(2002.9.27)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｌ　9/10		Ｇ０６Ｆ　15/00	３３０Ｃ	５Ｂ０３５
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｋ　17/00	Ｓ	５Ｂ０５８
Ｇ０６Ｋ　17/00		Ｈ０４Ｌ　9/00	６２１Ａ	５Ｂ０８５
19/10		Ｇ０６Ｋ　19/00	Ｒ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ	

審査請求　未請求　請求項の数６　ＯＬ　（全　９　頁）

(21)出願番号　特願2001－82054(P2001－82054)

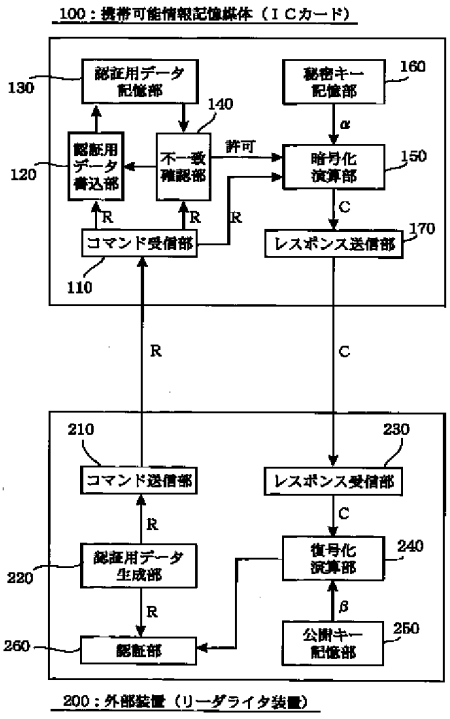
(22)出願日　平成13年３月22日(2001.3.22)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　神力　哲夫
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　入澤　和義
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100091476
弁理士　志村　浩

最終頁に続く

(54)【発明の名称】　携帯可能情報記憶媒体およびその認証方法

(57)【要約】
【課題】　ＩＣカード内の暗号化演算時の消費電力等を観測して統計的手法により非破壊的に秘密キーを推測する不正な解析手法の実施を困難にする。
【解決手段】　リーダライタ装置２００で発生させた乱数からなる認証用データＲをＩＣカード１００に与え、秘密キーαを利用して暗号化し、暗号データＣとして戻してもらう。この暗号データＣを公開キーβを利用して復号化してＩＣカードの認証を行う。認証用データ記憶部１３０内に、過去に与えられた認証用データＲを蓄積しておくようにし、新たな認証用データＲが過去のデータと同一の場合、暗号化演算を実行しないようにし、同一の認証用データＲを繰り返し与えることによる不正な統計的解析手法を不可能にする。



1

【特許請求の範囲】

【請求項１】　外部装置から携帯可能情報記憶媒体に対するアクセスを行う際に、前記携帯可能情報記憶媒体が正しいものであることを確認する認証方法であって、

任意の認証用データＲに対して、第１のキーαを用いた暗号化演算を行うことにより暗号データＣが得られ、かつ、この暗号データＣに対して、第２のキーβを用いた復号化演算を行うことにより前記認証用データＲと同一のデータが得られるように、第１のキーαおよび第２のキーβ、ならびに暗号化演算および復号化演算を定める演算定義段階と、

前記携帯可能情報記憶媒体内に前記第１のキーαを記憶させるとともに、前記携帯可能情報記憶媒体に前記暗号化演算を行う処理機能を準備する媒体準備段階と、

前記外部装置において乱数を発生させ、この乱数を認証用データＲとして前記携帯可能情報記憶媒体に送信する乱数送信段階と、

認証用データＲの送信を受けて、これを前記携帯可能情報記憶媒体内の所定の記憶場所に記憶させる認証用データ記憶段階と、

前記携帯可能情報記憶媒体内において、新たに送信されてきた認証用データＲが、これまでに記憶されている認証用データＲと一致するか否かを調べ、いずれとも不一致の場合に暗号化許可なる判定を行う判定段階と、

前記判定段階において暗号化許可なる判定が行われた場合に、前記携帯可能情報記憶媒体内において、送信されてきた認証用データＲに対して、記憶している前記第１のキーαを用いた前記暗号化演算を実行させ、その結果得られる暗号データＣを前記外部装置に返信させる暗号化段階と、

前記外部装置において、前記携帯可能情報記憶媒体から返信された暗号データＣに対して、前記第２のキーβを用いた前記復号化演算を実行させる復号化段階と、

前記復号化演算の結果、前記乱数送信段階で送信した認証用データＲと同一のデータが得られた場合に、前記携帯可能情報記憶媒体を正しいものと確認する認証段階と、

を有することを特徴とする携帯可能情報記憶媒体の認証方法。

【請求項２】　請求項１に記載の認証方法において、

乱数送信段階によって送信された認証用データＲについて、認証用データ記憶段階に先立って判定段階を行い、この判定段階において暗号化許可なる判定結果が得られた場合にのみ、認証用データ記憶段階を実行するようにしたことを特徴とする携帯可能情報記憶媒体の認証方法。

【請求項３】　請求項１または２に記載の認証方法において、

携帯可能情報記憶媒体内に、認証用データＲを記憶することが可能な複数ｎ個の記憶場所を用意し、認証用データ記憶段階では、最近ｎ回分の認証用データＲのみを記憶させるようにしたことを特徴とする携帯可能情報記憶媒体の認証方法。

2

【請求項４】　外部装置から認証コマンドとともに認証用データＲが送信されてきたときに、この認証用データＲに対して所定の暗号化演算を実行し、その結果得られる暗号データＣをレスポンスとして前記外部装置に返信する機能をもった携帯可能情報記憶媒体であって、

前記外部装置から送信されるコマンドを受信するコマンド受信部と、

前記認証用データＲを記憶するための認証用データ記憶部と、

前記暗号化演算に利用するための秘密キーαを記憶するための秘密キー記憶部と、

前記コマンド受信部が、認証コマンドとともに認証用データＲを受信したときに、前記認証用データ記憶部内に記憶されている認証用データＲと、新たに受信した認証用データＲとが不一致であることを確認する不一致確認部と、

前記コマンド受信部が受信した認証用データＲを、前記認証用データ記憶部に書き込む認証用データ書込部と、

前記不一致確認部において不一致が確認されたことを条件として、前記秘密キー記憶部内に記憶されている秘密キーαを用いて、新たに受信した認証用データＲに対して暗号化演算を実行して暗号データＣを得る暗号化演算部と、

前記暗号データＣを含むレスポンスを前記外部装置に送信するレスポンス送信部と、

を備えることを特徴とする携帯可能情報記憶媒体。

【請求項５】　請求項４に記載の携帯可能情報記憶媒体において、

新たに受信した認証用データＲについて、不一致確認部において不一致が確認されたことを条件として、認証用データ書込部における前記新たに受信した認証用データＲの書き込みが行われるようにしたことを特徴とする携帯可能情報記憶媒体。

【請求項６】　請求項４または５に記載の携帯可能情報記憶媒体において、

認証用データ記憶部に、複数ｎ通りの認証用データＲを記憶することができるように複数ｎ個の記憶場所を用意し、

認証用データ書込部は、書込対象となる認証用データＲを各記憶場所に順次書き込む処理を実行し、複数ｎ個の記憶場所が既にすべて書き込み済みとなっていた場合には、最も古い認証用データＲが書き込まれている記憶場所に対する書き換え処理を実行することを特徴とする携帯可能情報記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯可能情報記憶

媒体およびその認証方法に関し、特に、ＩＣカードに対して外部装置からアクセスする際に、このＩＣカードが正しいものであることを認証するための認証方法およびそのような認証方法を行うのに適したＩＣカードに関する。

【０００２】

【従来の技術】ＩＣカードに代表される携帯可能情報記憶媒体は、ＩＣチップの小型化技術とともに急速に普及しつつあり、一般の個人ユーザにまで１枚ずつ行き渡るようになるのも、もはや時間の問題である。このように、ＩＣカード等の携帯可能情報記憶媒体が、社会生活の基幹をなす道具として利用されるようになればなるほど、セキュリティの確保が重要な課題となってくる。ＩＣカードに対するアクセスには、いわゆるリーダライタ装置が利用され、コンピュータシステムは、このリーダライタ装置を介して、ＩＣカードの内部とデータのやりとりを行うことになる。そこで、通常は、リーダライタ装置にＩＣカードが挿入されると、相互に相手を認証する処理が行われる。

【０００３】リーダライタ装置側からＩＣカードを見て、当該ＩＣカードが正しいものであるか否かを確認するための認証は、通常、認証コマンドとともに任意の認証用データ（乱数が利用されている）をリーダライタ装置からＩＣカードへ与え、これに対する正しいレスポンスが返ってくるか否かを検証する、という方法によって行われている。より具体的には、公開鍵暗号方式を利用して、正規のＩＣカードには、内部に秘密キーαを格納しておき、リーダライタ装置側から与えた認証用データ（任意の乱数）に対して、ＩＣカード内部において、この秘密キーαを用いた暗号化処理を実施させ、この暗号化処理によって得られた暗号データをレスポンスとして戻させ、リーダライタ装置側では、このレスポンスとして返された暗号データに対して、秘密キーαに対応した公開キーβを用いた復号化処理を実行し、この復号化処理によって得られたデータが、もとの認証用データに一致するか否かによって、ＩＣカードに対する認証を行っている。

【０００４】ＩＣカード内に格納された秘密キーαは、通常、どのような方法によっても外部へは読み出されない構造となっているため、正しい秘密キーαを有するＩＣカードを偽造することは極めて困難である。したがって、上述した方法によって、暗号データをレスポンスとして返させ、これを復号化することにより得られたデータが、元の認証用データと一致すれば、当該ＩＣカードは正規のものであるとの認証が得られる。

【０００５】

【発明が解決しようとする課題】上述したように、ＩＣカード内に格納された秘密キーαは、論理的には、どのような方法によっても外部へは読み出されない仕組みになっている。しかしながら、現実的には、ＩＣカード動作中の様々な物理現象（たとえば消費電流）を解析することで、非破壊的に、ＩＣカード内に格納されている秘密キーαを外部から検知する方法が存在する。たとえば、ＤＰＡ（Differential Power Analysis）と呼ばれている手法は、ＩＣカードの消費電力の波形を統計的に解析することにより、秘密キーαの内容を推測するという原理に基づいている。具体的には、ＩＣカードの電力供給用端子などに、ＩＣカード内部における消費電流を測定するための測定系を接続した状態にし、リーダライタ装置側から所定の認証用データを繰り返し送信して、ＩＣカード内部で秘密キーαを用いた暗号化演算を実行し、このときの消費電力波形を解析することにより、統計的な手法で秘密キーαの内容を把握する。

【０００６】そこで本発明は、上述したような不正な解析手法に対しても十分なセキュリティを確保することが可能な携帯可能情報記憶媒体の認証方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】(1)　本発明の第１の態様は、外部装置から携帯可能情報記憶媒体に対するアクセスを行う際に、この携帯可能情報記憶媒体が正しいものであることを確認する認証方法において、任意の認証用データＲに対して、第１のキーαを用いた暗号化演算を行うことにより暗号データＣが得られ、かつ、この暗号データＣに対して、第２のキーβを用いた復号化演算を行うことにより元の認証用データＲと同一のデータが得られるように、第１のキーαおよび第２のキーβ、ならびに暗号化演算および復号化演算を定める演算定義段階と、携帯可能情報記憶媒体内に第１のキーαを記憶させるとともに、この携帯可能情報記憶媒体に暗号化演算を行う処理機能を準備する媒体準備段階と、外部装置において乱数を発生させ、この乱数を認証用データＲとして携帯可能情報記憶媒体に送信する乱数送信段階と、認証用データＲの送信を受けて、これを携帯可能情報記憶媒体内の所定の記憶場所に記憶させる認証用データ記憶段階と、携帯可能情報記憶媒体内において、新たに送信されてきた認証用データＲが、これまでに記憶されている認証用データＲと一致するか否かを調べ、いずれとも不一致の場合に暗号化許可なる判定を行う判定段階と、この判定段階において暗号化許可なる判定が行われた場合に、携帯可能情報記憶媒体内において、送信されてきた認証用データＲに対して、記憶している第１のキーαを用いた暗号化演算を実行させ、その結果得られる暗号データＣを外部装置に返信させる暗号化段階と、外部装置において、携帯可能情報記憶媒体から返信された暗号データＣに対して、第２のキーβを用いた復号化演算を実行させる復号化段階と、この復号化演算の結果、乱数送信段階で送信した認証用データＲと同一のデータが得られた場合に、携帯可能情報記憶媒体を正しいものと確認する認証段階と、を行うようにしたものである。

【０００８】(2)　本発明の第２の態様は、上述の第１の態様に係る携帯可能情報記憶媒体の認証方法において、乱数送信段階によって送信された認証用データＲについて、認証用データ記憶段階に先立って判定段階を行い、この判定段階において暗号化許可なる判定結果が得られた場合にのみ、認証用データ記憶段階を実行するようにしたものである。

【０００９】(3)　本発明の第３の態様は、上述の第１または第２の態様に係る携帯可能情報記憶媒体の認証方法において、携帯可能情報記憶媒体内に、認証用データＲを記憶することが可能な複数ｎ個の記憶場所を用意し、認証用データ記憶段階では、最近ｎ回分の認証用データＲのみを記憶させるようにしたものである。

【００１０】(4)　本発明の第４の態様は、外部装置から認証コマンドとともに認証用データＲが送信されてきたときに、この認証用データＲに対して所定の暗号化演算を実行し、その結果得られる暗号データＣをレスポンスとして外部装置に返信する機能をもった携帯可能情報記憶媒体において、外部装置から送信されるコマンドを受信するコマンド受信部と、認証用データＲを記憶するための認証用データ記憶部と、暗号化演算に利用するための秘密キーαを記憶するための秘密キー記憶部と、コマンド受信部が、認証コマンドとともに認証用データＲを受信したときに、認証用データ記憶部内に記憶されている認証用データＲと、新たに受信した認証用データＲとが不一致であることを確認する不一致確認部と、コマンド受信部が受信した認証用データＲを、認証用データ記憶部に書き込む認証用データ書込部と、不一致確認部において不一致が確認されたことを条件として、秘密キー記憶部内に記憶されている秘密キーαを用いて、新たに受信した認証用データＲに対して暗号化演算を実行して暗号データＣを得る暗号化演算部と、暗号データＣを含むレスポンスを外部装置に送信するレスポンス送信部と、を設けるようにしたものである。

【００１１】(5)　本発明の第５の態様は、上述の第４の態様に係る携帯可能情報記憶媒体において、新たに受信した認証用データＲについて、不一致確認部において不一致が確認されたことを条件として、認証用データ書込部における新たに受信した認証用データＲの書き込みが行われるようにしたものである。

【００１２】(6)　本発明の第６の態様は、上述の第４または第５の態様に係る携帯可能情報記憶媒体において、認証用データ記憶部に、複数ｎ通りの認証用データＲを記憶することができるように複数ｎ個の記憶場所を用意し、認証用データ書込部が、書込対象となる認証用データＲを各記憶場所に順次書き込む処理を実行し、複数ｎ個の記憶場所が既にすべて書き込み済みとなっていた場合には、最も古い認証用データＲが書き込まれている記憶場所に対する書き換え処理を実行するようにしたものである。

【００１３】

【発明の実施の形態】以下、本発明を図示する実施形態に基づいて説明する。はじめに、図１のブロック図を参照しながら、従来の一般的な携帯可能情報記憶媒体（具体的には、ＩＣカード）において行われている認証方法の基本原理を説明する。この認証方法は、秘密鍵と公開鍵とからなるペア鍵を利用する公開鍵暗号方式を利用した認証方法である。

【００１４】図１は、携帯可能情報記憶媒体（ＩＣカード）１００を、外部装置（リーダライタ装置）２００に挿入し、両者を電気的に接続した状態において、リーダライタ装置２００側から、ＩＣカード１００側を認証する手順を示すブロック図である。図示の例では、ＩＣカード１００内には、予め第１のキーα（秘密キー）が格納されており、リーダライタ装置２００内には、予め第２のキーβ（公開キー）が格納されている。ここで、第１のキーαは、たとえば、このＩＣカード１００の所有者に固有のキーであり、一般には知らされていない秘密のキーとなっている。これに対して、第２のキーβは、同じくこの所有者に固有のキーではあるが、一般に公開されたキーとなっている。したがって、第２のキーβは、リーダライタ装置２００内に常に格納しておかなくても、その都度、別な場所（たとえば、ホストコンピュータなど）からリーダライタ装置２００内に読み込むようにしてもかまわない。また、ＩＣカード１００には、第１のキーαを利用して、任意のデータに対する暗号化処理を実行する機能が備わっており、リーダライタ装置２００には、第２のキーβを利用して、任意の暗号データに対する復号化処理を実行する機能が備わっている。

【００１５】また、リーダライタ装置２００には、乱数を発生させる機能が備わっており、リーダライタ装置２００で発生された乱数は、認証用データＲとして、認証コマンドとともに、ＩＣカード１００側へ送信されることになる。ＩＣカード１００側では、こうして送信されてきた認証用データＲに対して、第１のキーαを用いて暗号化演算を実行することにより、暗号データＣを生成することができる。暗号データＣは、第１のキーαを用いるという前提において、認証用データＲに基づいて一義的に求まるデータである。ＩＣカード１００は、こうして求めた暗号データＣを、認証コマンドに対するレスポンスとして、リーダライタ装置２００へと返信する。リーダライタ装置２００側では、こうして送信されてきた暗号データＣに対して、第２のキーβを用いて復号化演算を実行する。そして、この復号化演算によって得られたデータが、元の認証用データＲに一致すれば、ＩＣカード１００を正しいものとして認証することになる。

【００１６】もちろん、このような認証方法を可能にするためには、予め、第１のキーαおよび第２のキーβならびに暗号化演算および復号化演算を、特定のものに定めておく必要がある。すなわち、任意の認証用データＲ

に対して、第１のキーαを用いた暗号化演算を行うことにより暗号データＣが得られ、かつ、この暗号データＣに対して、第２のキーβを用いた復号化演算を行うことにより前記認証用データＲと同一のデータが得られるように、第１のキーαおよび第２のキーβならびに暗号化演算および復号化演算を定めておかねばならない。別言すれば、第１のキーαと第２のキーβとは、公開鍵暗号方式における秘密鍵と公開鍵とに相当するペア鍵の関係になっている必要があり、ＩＣカード１００側で行われる暗号化演算およびリーダライタ装置２００側で行われる復号化演算は、この公開鍵暗号方式における暗号化演算および復号化演算になっている必要がある。

【００１７】リーダライタ装置２００側で発生させる認証用データＲとしては、乱数が用いられるので、ＩＣカード１００側に与えられる認証用データＲの内容は毎回異なることになる。したがって、ＩＣカード１００側からレスポンスとして返される暗号データＣの内容も毎回異なる。しかしながら、ＩＣカード１００側が正しい秘密キーαを用いて正しい暗号化演算を実施している限り、リーダライタ装置２００側で正しい公開キーβを用いて正しい復号化演算を行えば、復号化されたデータは元の認証用データＲに一致する。よって、元の認証用データＲがどのような値であっても、ＩＣカード１００に対する認証が可能になる。しかも、ＩＣカード１００内に格納されている秘密キーαは、論理的には、ＩＣカードの外部に読み出されることはないので、一応、十分なセキュリティが確保されているように見える。

【００１８】しかしながら、実際には、既に述べたように、ＩＣカードの消費電流を統計的に解析する手法を利用すると、ＩＣカード１００内の秘密キーαの内容を外部から察知することが可能になる。たとえば、「１１１１１１１１」なる認証用データＲを、何度も繰り返してＩＣカード１００に与え、そのときのＩＣカード１００内部の消費電力波形を電気的な測定方法で繰り返して観測すると、統計的に何らかのパターンが得られることになる。同様に、「００００００００」なる認証用データＲを、何度も繰り返してＩＣカード１００に与え、そのときのＩＣカード１００内部の消費電力波形を電気的な測定方法で繰り返して観測すると、やはり統計的に何らかのパターンが得られることになる。このようなパターンを解析することにより、内部に格納されている秘密キーαの内容を統計的に類推することが可能になる。

【００１９】本発明の特徴は、このような不正な解析手法を困難にするために、ＩＣカード１００に対して、同一の認証用データＲが繰り返して与えられた場合には、ＩＣカード１００内部での暗号化演算を拒否するようにする、という点にある。たとえば、上述の例の場合、第１回目の認証コマンドにおいて、「１１１１１１１１」なる認証用データＲが与えられたとすると、この第１回目の認証コマンドに対しては、秘密キーαを用いた暗号化演算が実行され、得られた暗号データＣがレスポンスとして返信されることになるが、第２回目以降の認証コマンドにおいて、もし同一の「１１１１１１１１」なる認証用データＲが与えられた場合には、当該認証コマンドは拒否され、秘密キーαを用いた暗号化演算は実行されないことになる。もちろん、正常なレスポンスも得られない。

【００２０】このような仕組みにしておけば、同一の認証用データＲを用いた暗号化演算を繰り返し実行させることはできなくなるので、消費電力波形を統計的な手法で解析することは困難になる。

【００２１】このような目的を達成するためには、ＩＣカード１００の構成を、図２のブロック図に示すような構成にすればよい。この図２のブロック図は、本発明に係るＩＣカード１００（携帯可能情報記憶媒体）を、従来の一般的なリーダライタ装置２００（外部装置）に接続した状態を示している。図示のとおり、この実施形態に係るＩＣカード１００は、コマンド受信部１１０、認証用データ書込部１２０、認証用データ記憶部１３０、不一致確認部１４０、暗号化演算部１５０、秘密キー記憶部１６０、レスポンス送信部１７０を有している。一方、リーダライタ装置２００は、コマンド送信部２１０、認証用データ生成部２２０、レスポンス受信部２３０、復号化演算部２４０、公開キー記憶部２５０、認証部２６０を有している。もちろん、図２に図示されているのは、本発明に係る認証処理を実行するために必要な構成要素だけであり、実際のＩＣカードやリーダライタ装置には、ＩＣカードおよびリーダライタ装置としての本来の機能を実行するための他の構成要素も備わっている。

【００２２】図２に示すリーダライタ装置２００は、従来の一般的なリーダライタ装置であり、逆に言えば、本発明を実施する上で、リーダライタ装置は従来のものをそのまま利用することが可能である。認証用データ生成部２２０は、実際には乱数を発生させる手段であり、ここで発生させた乱数が、認証用データＲとしてＩＣカード１００側に与えられることになる。すなわち、乱数として発生された認証用データＲは、コマンド送信部２１０から、認証コマンドとともにコマンド受信部１１０へ向けて送信される。ＩＣカード１００は、こうして認証コマンドとともに認証用データＲが送信されてきたときに、この認証用データＲに対して所定の暗号化演算を実行し、その結果得られる暗号データＣをレスポンスとして返信する機能をもった携帯可能情報記憶媒体であり、レスポンスとしての暗号データＣは、レスポンス送信部１７０からレスポンス受信部２３０へ向けて送信されることになる。

【００２３】リーダライタ装置２００側では、こうして返信されてきた暗号データＣに対する復号化演算を行う。すなわち、公開キー記憶部２５０に格納されている

公開キーβを用いて、復号化演算部２４０において、暗号データＣに対する復号化演算を行う。この演算結果として得られた復号データは、認証部２６０において、認証用データ生成部２２０が生成した元の認証用データＲと比較され、両者が一致した場合に、ＩＣカード１００が正しいものであるとの認証が行われる点は、既に述べたとおりである。

【００２４】一方、ＩＣカード１００側で行われる暗号化演算の処理も、基本的には、既に述べたとおりである。すなわち、コマンド受信部１１０で受信された認証用データＲは、暗号化演算部１５０に与えられて暗号化される。秘密キー記憶部１６０には、秘密キーαが格納されている。暗号化演算部１５０は、この秘密キー記憶部１６０から秘密キーαを読み出し、これを利用して、認証用データＲに対する暗号化演算を実行し、暗号データＣを求める処理を行う。求まった暗号データＣは、レスポンス送信部１７０からレスポンスとして送信される。

【００２５】ただし、暗号化演算部１５０がこの暗号化演算を行うためには、不一致確認部１４０からの許可が必要とされる。別言すれば、コマンド受信部１１０に認証用データＲが与えられたとしても、不一致確認部１４０から、この認証用データＲについての暗号化演算を許可する旨の信号が与えられない限り、暗号化演算部１５０は暗号化演算を行わないことになる。不一致確認部１４０は、コマンド受信部１１０に新たに与えられた認証用データＲが、過去に与えられた認証用データＲに一致するか否かを判定し、不一致であった場合にのみ、暗号化演算部１５０に対して暗号化演算を許可する旨の信号を与える。不一致確認部１４０に、このような判定を行わせるためには、これまで与えられた認証用データＲを蓄積しておく必要がある。このような蓄積処理は、認証用データ書込部１２０および認証用データ記憶部１３０によって行われる。認証用データ記憶部１３０は、これまでに与えられた複数の認証用データＲを蓄積記憶するための記憶場所を有しており、認証用データ書込部１２０は、コマンド受信部１１０が受信した認証用データＲを、この認証用データ記憶部１３０に順次書き込む処理を行う。

【００２６】もちろん、このＩＣカード１００を初めて使用するときには、認証用データ記憶部１３０内にはまだ認証用データＲは蓄積されていないが、コマンド送信部２１０から認証コマンドとともに認証用データＲが送信されてくるたびに、認証用データ書込部１２０によって、この認証用データＲが認証用データ記憶部１３０へと書き込まれることになる。不一致確認部１４０は、コマンド受信部１１０が、認証コマンドとともに認証用データＲを受信したときに、認証用データ記憶部１３０内に記憶されている認証用データＲと、新たに受信した認証用データＲとが不一致であることを確認して、暗号化演算部１５０に対して暗号化演算を許可する旨の信号を与えることになる。暗号化演算部１５０は、この不一致確認部１４０において不一致が確認されたことを条件として、秘密キー記憶部１６０内に記憶されている秘密キーαを用いて、新たに受信した認証用データＲに対して暗号化演算を実行して暗号データＣを得る演算を実行する。

【００２７】なお、この実施形態では、認証用データ書込部１２０は、新たに受信した認証用データＲについて、不一致確認部１４０において不一致が確認されたことを条件として、この新たに受信した認証用データＲの書き込みを行うようにしている。すなわち、コマンド受信部１１０に認証コマンドとともに新たな認証用データＲが受信されたとき、まず、不一致確認部１４０による不一致確認の処理が実行され、不一致が確認されたときにのみ、認証用データ書込部１２０によって当該認証用データＲが認証用データ記憶部１３０に書き込まれることになる。逆に言えば、もし不一致確認部１４０において一致が確認された場合には、当該認証用データＲは、認証用データ書込部１２０によって書き込まれることはない。このような運用は、認証用データ記憶部１３０内のデータから冗長性を排除する上で意味がある。すなわち、既に認証用データ記憶部１３０内に記憶されているデータと同一のデータについては、再度の書き込みが行われることはない。

【００２８】また、実用上、ＩＣカード１００内のメモリ容量は有限であり、当然、認証用データ記憶部１３０の記憶容量も有限である。したがって、ＩＣカード１００が長期間利用され、何度もリーダライタ装置２００へと挿入されて認証を受けることになると、認証用データ記憶部１３０内の空領域は徐々に減少してゆき、やがて全領域に認証用データＲが書き込まれた状態になってしまう。このような場合には、認証用データ記憶部１３０内には、最近の認証用データＲのみを残し、古いデータから書き換えるような処理を行えばよい。たとえば、認証用データ記憶部１３０内に、認証用データＲを記憶することが可能な複数ｎ個の記憶場所が用意されていた場合、最近ｎ回分の認証用データＲのみが記憶された状態になるようにすればよい。すなわち、空領域がなくなるまでは、書込対象となる認証用データＲを各記憶場所に順次書き込む処理を実行し、複数ｎ個の記憶場所が既にすべて書き込み済みとなった後は、最も古い認証用データＲが書き込まれている記憶場所に対する書き換え処理を実行すればよい。

【００２９】図３は、このような書き換え処理の一例を示す図である。まず、図３(a) に示すように、記憶場所番号１～ｎで示される複数ｎ個の記憶場所が用意されている場合に、３つの認証用データＲ（１），Ｒ（２），Ｒ（３）が順次与えられたとすると、これらのデータは、図示のとおり記憶場所番号１，２，３へと順次書き

込まれることになる。ここでは、最後の書込場所を、ポインタＰで示すことができるようにしてある。続いて、たとえば、新たな認証用データＲ（４）が与えられた場合には、ポインタＰが指し示す最後の書込場所の次に位置する記憶場所番号４への書き込みを行い、ポインタＰを更新すればよい。図３(b) は、このようにして順次書き込みを行ってゆき、合計ｎ個の認証用データＲ（１）～Ｒ（ｎ）がすべて書き込まれた状態を示している。この状態において、更に次の認証用データＲ（ｎ＋１）が与えられた場合には、図３(c) に示すように、最も古い認証用データＲ（１）が書き込まれていた記憶場所番号１の位置に対する書き換えを行えばよい。図３(d) は、更に、新たな認証用データＲ（ｎ＋２），Ｒ（ｎ＋３）が与えられた場合の書込状態を示している。このような書換処理を行えば、常に、最新のｎ個の認証用データが蓄積記憶されることになる。

【００３０】図４は、本発明に係る携帯可能情報記憶媒体の認証方法の手順を示す流れ図である。もちろん、この図４に示す手順を実施する際には、所定の秘密キーαが格納され、この秘密キーαを用いて所定の暗号化演算を実行する機能をもった携帯可能情報記憶媒体（ＩＣカード１００）を準備しておく必要があり、これにアクセスするための外部装置（リーダライタ装置２００）を準備しておく必要がある。

【００３１】さて、ＩＣカード１００がリーダライタ装置２００に挿入されると、まず、ステップＳ１において、リーダライタ装置２００側で認証用データＲ（乱数）が発生され、続くステップＳ２において、この認証用データＲがＩＣカード１００側へと送信される。実際には、上述したように、認証コマンドとともに認証用データＲがＩＣカード１００側へと与えられることになる。ＩＣカード１００は、ステップＳ３において、この認証用データＲを受信したら、続くステップＳ４において、過去ｎ回分の認証用データＲとの一致判定が行われる（もちろん、認証用データ記憶部１３０内にまだｎ回分の認証用データＲが蓄積されていない場合には、これまでに蓄積されている認証用データＲとの一致判定を行えばよい）。

【００３２】ここで、蓄積されている認証用データＲのいずれとも不一致である旨の判定がなされたら、ステップＳ５からステップＳ６へと進み、この新たに受信された認証用データＲを、認証用データ記憶部１３０へと書き込む処理が行われる。このように、ステップＳ６の認証用データの書込処理に先立って、ステップＳ４の一致判定を行い、不一致なる判定結果が得られた場合にのみ、ステップＳ６の書込処理を行うようにするのは、前述したように、認証用データ記憶部１３０内に蓄積される認証用データＲの冗長性を排除するため（同一のデータが重複して書き込まれないようにするため）である。次に、ステップＳ７において、この認証用データＲに対して、秘密キーαを用いた暗号化演算が実行され、得られた暗号データＣが、ステップＳ８において、レスポンスとして送信される。

【００３３】リーダライタ装置２００は、ステップＳ９において、このレスポンスとして送信された暗号データＣを受信し、ステップＳ１０において、この暗号データＣに対して、公開キーβを用いた復号化演算を実行する。そして、ステップＳ１１において、この復号化演算の結果として得られた復号データと、元の認証用データＲ（ステップＳ１で発生した乱数）との一致を判定する。両者が一致していれば、ステップＳ１２からステップＳ１３へと進み認証成功となり、両者が一致していなければ、ステップＳ１２からステップＳ１４へと進み認証失敗となる

【００３４】一方、ＩＣカード１００側において実施されたステップＳ４の一致判定の結果、認証用データ記憶部１３０内に蓄積されていたいずれかの認証用データＲと一致する結果が得られたら、ステップＳ５からステップＳ１５へと進み、リーダライタ装置２００に対するレスポンスとして、エラーの送信が行われる。この場合、リーダライタ装置２００は、ステップＳ１６において、レスポンスとしてエラーを受信することになるので、続くステップＳ１７において、所定のエラー処理を行うようにする。

【００３５】このような手順でＩＣカード１００に対する認証を行うようにすれば、ステップＳ４における判定において、新たに与えられた認証用データＲが過去ｎ回分の認証用データＲとは不一致の場合に限って、ステップＳ７における暗号化演算が実行されることになるので、同一の認証用データＲをＩＣカード１００に繰り返して与え、そのときの消費電力を繰り返し観測し、統計的な手法により秘密キーαを類推するという不正な解析手法の実施を困難にすることができる。

【００３６】以上、本発明を図示する実施形態に基づいて説明したが、本発明はこの実施形態に限定されるものではなく、この他にも種々の形態で実施可能である。たとえば、上述の実施形態では、リーダライタ装置を介してＩＣカードに対する認証を行う例を述べたが、本発明は、一般的な携帯可能情報記憶媒体に対して、外部装置から認証を行う場合に広く適用可能である。

【００３７】

【発明の効果】以上のとおり本発明に係る携帯可能情報記憶媒体の認証方法によれば、不正な解析手法に対しても十分なセキュリティを確保することが可能になる。

【図面の簡単な説明】

【図１】携帯可能情報記憶媒体（ＩＣカード）１００を、外部装置（リーダライタ装置）２００に挿入し、両者を電気的に接続した状態において、リーダライタ装置２００側から、ＩＣカード１００側を認証する手順を示すブロック図である。

【図２】本発明に係る携帯可能情報記憶媒体（ＩＣカード）１００を、外部装置（リーダライタ装置）２００に接続した状態における両者の構成要素を示すブロック図である。

【図３】図２に示す携帯可能情報記憶媒体（ＩＣカード）１００内の認証用データ記憶部１３０の構成例および認証用データの格納例を示す図である。

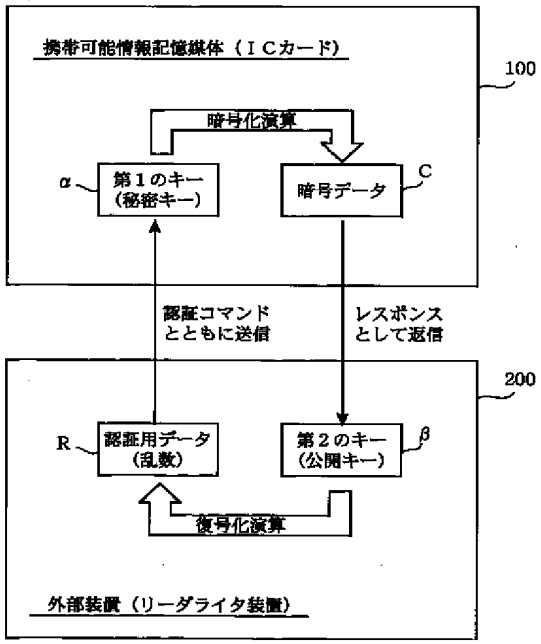
【図４】本発明に係る携帯可能情報記憶媒体の認証方法の基本手順を示す流れ図である。

【符号の説明】

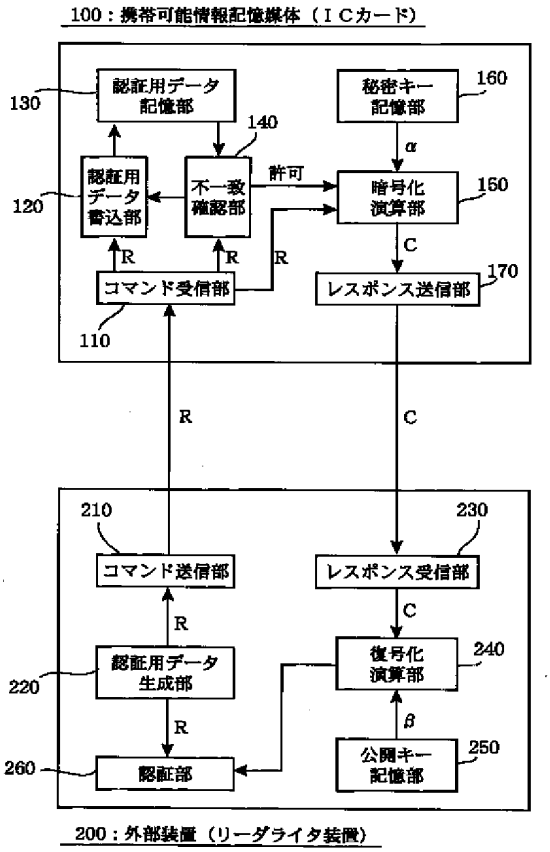
１００…携帯可能情報記憶媒体（ＩＣカード）
１１０…コマンド受信部
１２０…認証用データ書込部
１３０…認証用データ記憶部
１４０…不一致確認部
１５０…暗号化演算部

１６０…秘密キー記憶部
１７０…レスポンス送信部
２００…外部装置（リーダライタ装置）
２１０…コマンド送信部
２２０…認証用データ生成部
２３０…レスポンス受信部
２４０…復号化演算部
２５０…公開キー記憶部
２６０…認証部
Ｃ…暗号データ
Ｐ…ポインタ
Ｒ…認証用データ（乱数）
Ｒ（１）～Ｒ（ｎ＋３）…認証用データ（乱数）
α…第１のキー（秘密キー）
β…第２のキー（公開キー）

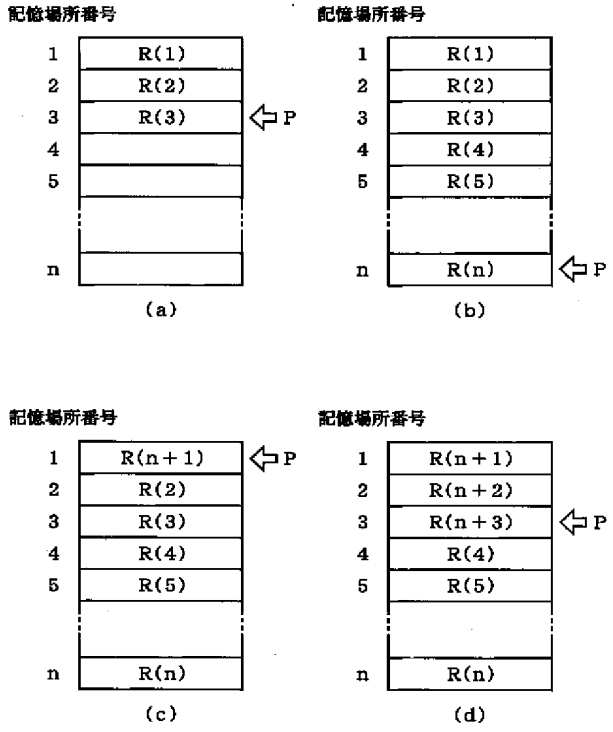
【図１】



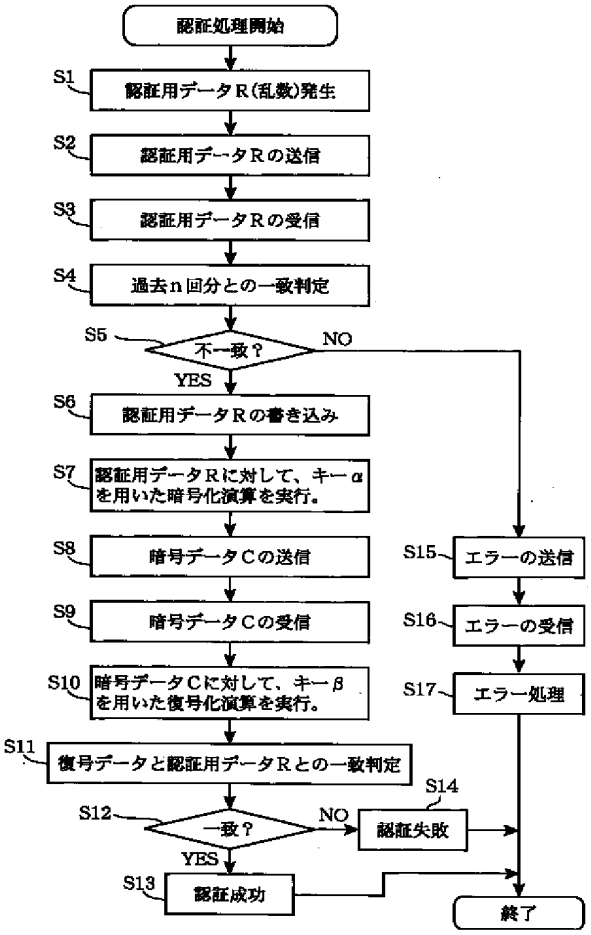
【図２】



【図３】



【図４】



フロントページの続き

(72)発明者　柴田　直人
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

Ｆターム(参考)　5B035 AA13 BB09 CA11 CA38
5B058 CA27 KA02 KA04 KA08 KA31
KA35 YA20
5B085 AE00
5J104 AA07 AA16 AA47 EA15 GA05
KA02 KA05 KA06 KA21 NA02
NA35 NA37 NA40